

DIALOG(R)File 352:Derwent WPI

(c) 2001 Derwent Info Ltd. All rts. reserv.

013690285 \*\*Image available\*\*

WPI Acc No: 2001-174509/200118

XRPX Acc No: N01-126391

IC card identification with fingerprints involves operating card reader interface circuit to exchange card information in memory to host computer, when IC card owner is legitimate by analyzing his fingerprints

Patent Assignee: SHEN M X (SHEN-I)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2001005945	A	20010112	JP 99229629	A	19990816	200118 B

Priority Applications (No Type Date): TW 99U209054 U 19990603

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 2001005945	A	7	G06K-019/10	

Abstract (Basic): JP 2001005945 A

NOVELTY - The fingerprint of the IC card owner is scanned by sensor (12) and then the scanned data is compared with the data in memory (11). When the IC card owner is judged to be a legitimate user, based on the comparison result, the microprocessor (14) operates the card reader interface circuit (13) in order to exchange card information via card reader (2) to host computer (3) from memory (11).

USE - In cash transaction security when using credit card, money card etc., for identification of IC card using fingerprints of IC card.

ADVANTAGE - The risk accompanying when the IC card is lost or forgot, is reduced as the IC cards are used only after confirming whether the user is a legitimate user.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of IC card identifier apparatus.

Card reader (2)  
Host computer (3)  
Memory (11)  
Sensor (12)  
Card reader interface circuit (13)  
Microprocessor (14)  
pp; 7 DwgNo 1/5

Title Terms: IC; CARD; IDENTIFY; FINGERPRINT; OPERATE; CARD; READ;  
INTERFACE; CIRCUIT; EXCHANGE; CARD; INFORMATION; MEMORY; HOST; COMPUTER;  
IC; CARD; OWNER; FINGERPRINT

Derwent Class: T01; T04

International Patent Class (Main): G06K-019/10

International Patent Class (Additional): G06F-019/00; G06K-017/00;  
G06K-019/07

File Segment: EPI

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-5945

(P2001-5945A)

(43) 公開日 平成13年1月12日 (2001.1.12)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

ターム(参考)

G 0 6 K 19/10

G 0 6 K 19/00

S 5 B 0 3 5

G 0 6 F 19/00

17/00

V 5 B 0 5 5

G 0 6 K 17/00

G 0 6 F 15/30

3 3 0

5 B 0 5 8

19/07

3 5 0 Z

G 0 6 K 19/00

J

審査請求 有

請求項の数18 O L (全 7 頁)

(21) 出願番号

特願平11-229629

(22) 出願日

平成11年8月16日 (1999.8.16)

(31) 優先権主張番号

8 8 2 0 9 0 5 4

(32) 優先日

平成11年6月3日 (1999.6.3)

(33) 優先権主張国

台湾 (TW)

(71) 出願人 599114885

沈 明 祥

台湾雲林縣斗南鎮新崙路15号

(72) 発明者 沈 明 祥

台湾雲林縣斗南鎮新崙路15号

(74) 代理人 100060069

弁理士 奥山 尚男 (外3名)

Fターム(参考) 5B035 AA14 BB09 BC01

5B055 EE02 EE03 HB02 JJ02 JJ05

KK05

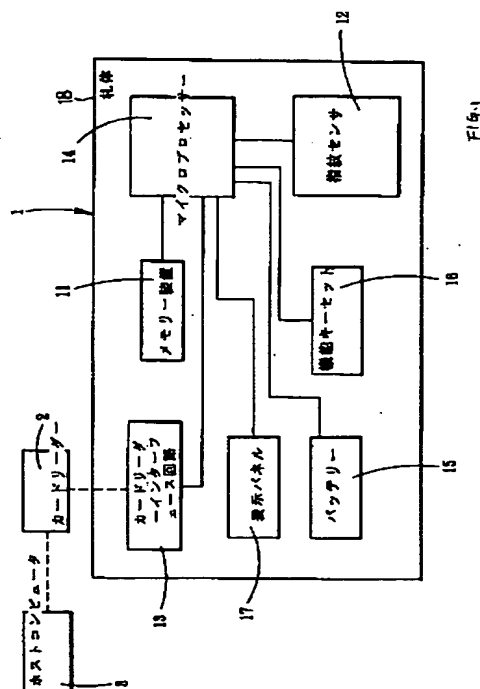
5B058 KA38

(54) 【発明の名称】 指紋によって識別されるICカード

(57) 【要約】

【課題】 カード紛失や置忘れによる危険性を低めて、インターネット取引上における安全性及び便利性を向上させるようにした、指紋によって識別されるICカードを提供する。

【解決手段】 ホストコンピュータ3と通信リンクを形成するカードリーダー2によりアクセスされるICカード1であって、礼体18と、この礼体18にそれぞれ設けられるメモリー装置11、指紋センサ12、及びカードリーダーインターフェース回路13と、指紋センサ12から受取った指紋走査データをメモリー装置11で指紋照合データと比較して、礼体18の所有者が正当使用者であると確認すれば、カードリーダーインターフェース回路13を作動してカードリーダー2を介してホストコンピュータ3とカード情報を交換するマイクロプロセッサ14とをそれぞれ備える。



## 【特許請求の範囲】

【請求項1】 ホストコンピュータと通信リンクを形成するカードリーダーによりアクセスされるICカードであって、

札体と、

上記札体に設けられて、正当使用者の指紋を走査して得られた指紋照合データ、及びカード情報を記憶するメモリ装置と、

上記札体に設けられて、上記札体所有者の指紋を走査して指紋走査データを生成する指紋センサと、

上記札体に設けられて、カードリーダーと通信するように作動できるカードリーダーインターフェース回路と、

上記札体に設けられて、上記メモリ装置、指紋センサ、及びカードリーダーインターフェース回路に接続され、上記指紋センサから受取った指紋走査データを上記メモリ装置で上記指紋照合データと比較して、上記札体の所有者が正当使用者であると確認した場合は、上記カードリーダーインターフェース回路を作動してカードリーダーを介してホストコンピュータとカード情報の交換をするマイクロプロセッサと、をそれぞれ具備することを特徴とする指紋によって識別されるICカード。

【請求項2】 上記指紋センサが指紋走査区域を区画した $m \times n$ 行列の走査セルを含むことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項3】 上記指紋走査データが上記走査セル配列の対応ラインを走査して得られた多数の走査線を含むことを特徴とする請求項2に記載の指紋によって識別されるICカード。

【請求項4】 上記走査セル配列の走査線が上記走査セル配列の行方向であることを特徴とする請求項3に記載の指紋によって識別されるICカード。

【請求項5】 上記走査セル配列の走査線が上記走査セル配列の列方向であることを特徴とする請求項3に記載の指紋によって識別されるICカード。

【請求項6】 上記各走査セルが、札体所有者の指紋の隆起紋を検出した場合は第1のロジックシグナルを発生して、札体所有者の指紋の谷底紋を検出した場合は第2のロジックシグナルを発生することを特徴とする請求項2に記載の指紋によって識別されるICカード。

【請求項7】 上記指紋照合データが多数の走査線データを含み、各走査線データが正当使用者の指紋のそれぞれ走査線指紋の特徴を記述してあることを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項8】 上記札体に設けられて上記マイクロプロセッサに接続された機能キーセットを備え、上記機能キーセットが上記ホストコンピュータとの交換カード情報を選択するようにしたことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項9】 上記札体に設けられて上記マイクロプロセッサに接続されて制御される表示パネルを備え、上

記ホストコンピュータと交換するカード情報を表示させるようにしたことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項10】 上記マイクロプロセッサが、上記札体所有者が正当使用者であると確認した状態の下で、上記メモリ装置が記憶している指紋照合データのセグメントを上記ホストコンピュータに伝送するようにしたことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項11】 上記マイクロプロセッサが、上記札体所有者が正当使用者であると確認した下で、上記メモリ装置が記憶している指紋照合データのセグメントをホストコンピュータに伝送するようにしたことを特徴とする請求項7に記載の指紋によって識別されるICカード。

【請求項12】 上記指紋照合データのセグメントが、上記ホストコンピュータと交換するカード情報の期日に対応して選択した走査線データの何れか一つを含むことを特徴とする請求項11に記載の指紋によって識別されるICカード。

【請求項13】 上記指紋照合データのセグメントが、上記ホストコンピュータと交換するカード情報の時間に対応して選択した走査線データの何れか一つを含むことを特徴とする請求項11に記載の指紋によって識別されるICカード。

【請求項14】 上記指紋照合データのセグメントが、ランダムに選択した走査線データの何れか一つを含むことを特徴とする請求項11に記載の指紋によって識別されるICカード。

【請求項15】 上記ホストコンピュータと交換するカード情報がクレジットカードナンバーを含むことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項16】 上記ホストコンピュータと交換するカード情報が銀行取引口座ナンバーを含むことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項17】 上記ホストコンピュータと交換するカード情報が正当使用者の身分証明カードナンバーを含むことを特徴とする請求項1に記載の指紋によって識別されるICカード。

【請求項18】 上記メモリ装置がフラッシュメモリであることを特徴とする請求項1に記載の指紋によって識別されるICカード。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ICカードに関し、特に、指紋を所有者と使用者の同定に利用するICカードに関する。

【0002】

【従来の技術】因みに、金融活動や科学技術の進歩に伴い、近年では、消費する際に大量の現金を持ち合せなくても、プラスチック通貨、例えばクレジットカード、キャッシュカード等を利用して購買を行える。この種のプラスチック通貨の利便性から、人々の携帯しているプラスチック通貨は、往々にして一枚だけに止まらず、且つその他のカード、例えば身分証明カードや出入証明カード等をも携帯するので、これらのカードが紛失でもすると、所有者は他人が冒認使用する危険に晒されることとなる。従って、このような危険の確率を最低限に抑えることができれば、所有者の損害を軽減することができる。そこで、例えば人間のそれぞれの指紋が異なることを利用して、これらのカードの所有者を識別できるようにすれば、カードが他人に悪用される可能性を最低限に低められる筈である。また、インターネットにより伝送した際に、しばしばデータがインターセプトされることがあって、近年流行っているインターネット上での取引において、カード関連データの伝送過程における安全性がますます重要視され、若しもインターネットでインターセプトされたデータが他人に使用され得ないのであれば、所有者にとって権益がより保障される筈である。なお、このように多数のカード、例えばクレジットカード、キャッシュカード、身分証明等を携帯して、もしもそのうちの何れかを使用する際は、往々にして多数のカードの中から探し出さなければならないので、不便で煩わしいばかりでなく、多数のカードが嵩張ってスペースを占めることとなるが、もしも一枚のカードでこれらカードに取って代れるものならば、生活上の利便性が一層向上する筈である。

【0003】

【発明が解決しようとする課題】本発明は、上記問題点に鑑みてなされたものであって、その目的は、カード紛失や置忘れによる危険性を低めて、インターネット取引における安全性及び利便性を向上させるようにした、指紋によって識別されるICカードを提供することにある。

【0004】

【課題を解決するための手段】上記目的を達成するため、本発明に係る指紋によって識別されるICカードは、ホストコンピュータとで通信リンクを形成するカードリーダーによってアクセスされ、上記ICカードが札体、上記札体に設けられるメモリ装置、上記札体に設けられる指紋センサ、上記札体に設けられるカードリーダーインターフェース回路、及び上記札体に設けられて上記メモリ装置、指紋センサ及びカードリーダーインターフェース回路に接続されるマイクロプロセッサを含んでおり、上記メモリ装置が正当使用者の指紋を走査して得られた指紋照合データ及びカード情報を記憶し、上記指紋センサが札体所有者の指紋を走査して指紋走査データを生成し、上記カードリーダーインターフェ

ース回路が作動してカードリーダーと通信できて、上記マイクロプロセッサが指紋センサから指紋走査データを受けると、上記指紋走査データとメモリ装置にある指紋照合データとを比較して、両方が一致すれば正当使用者が札体所有者であると判定し、上記カードリーダーインターフェース回路を作動してカードリーダーを介してホストコンピュータとカード情報を取り引するように構成される。

【0005】上記のように構成された本発明のICカードは、ICカード所有者の指紋を走査して得られた指紋走査データとメモリ装置に記憶された正当使用者の指紋照合データを比較して、正当使用者が所有者であると確認されてから使用できる。また、ICカードが時間や期日の関連条件を選択してなる指紋照合データのセグメントを伝送できるので、ホストコンピュータとの取引カード情報を機動的に変化させることができる。さらに、ICカード一枚でバンクカード、身分証明カード或いはクレジットカードとして使用できるので、単に一枚のカードだけを携帯して色々な役目を果たすることができる。

【0006】

【発明の実施の形態】以下、本発明を実施の形態に基づいて具体的に説明するが、本発明はこの例だけに限定されない。

【0007】図1は、本発明における比較的好ましい実施形態のブロック図で、図示の如く、本実施形態の指紋によって識別されるICカード1は、ホストコンピュータ3とで通信リンクを形成するカードリーダー(Card Reader)2によってアクセスされる。このカードリーダー2は、ほとんどがパブリックゾーン、例えば商店、デパートメント等に取付けられ、上記ホストコンピュータ3は、銀行、クレジットカードセンター等に設けられる。ICカード1は、札体18、及びこの札体18にそれぞれ取付けられるメモリ装置11、指紋センサ12、カードリーダーインターフェース回路13、マイクロプロセッサ14、バッテリー15、機能キーセット16及び表示パネル17を含んでいる。

【0008】上述のメモリ装置11は、フラッシュメモリ(FLASH MEMORY)であって、正当使用者またはカード体所有者の指紋を走査して得られた指紋照合データ及び正当使用者のデータ情報、例えば身分証明証ナンバー、銀行口座ナンバー、クレジットカードナンバー等を記憶しており、この指紋照合データは多数のそれぞれが正当使用者の指紋における各走査線の指紋の特徴を記述した走査線データを含んでいる。

【0009】上述の指紋センサ12は、正当使用者の指紋5(図2参照)を走査するものであり、正当使用者またはカード所有者の指紋5に対応する指紋走査データを生成する。図2に示す如く、この指紋センサ12は、 $m \times n$ 行列の走査セルを含んだ指紋走査区域Mを備えており、この指紋走査データは、多数の走査セルの行列ライ

ンを走査して得られた走査線データを含む。走査セルの行列ラインは、列方向或いは行方向の走査ができて、例えば、 $m=30$ 、 $n=45$ の場合、列方向の第1の走査線Iが(1,  $n$ ;  $n=1\sim45$ )で、列方向の第2の走査線IIが(2,  $n$ ;  $n=1\sim45$ )で、列方向の最後の走査線III、すなわち第30の走査線IIIが(30,  $n$ ;  $n=1\sim45$ )である。また、行方向の第1の走査線IVが( $m$ , 1;  $m=1\sim30$ )で、行方向の第2の走査線Vが( $m$ , 2;  $m=1\sim30$ )で、行方向の最後の走査線VI、即ち第45の走査線VIが( $m$ , 45;  $m=1\sim30$ )である。そして、札体18の所有者の指紋の隆起紋が検出されると、走査セルがハイ・ロジックシグナルを発生し、札体18の所有者の指紋の谷底紋が検出されると、走査セルがロー・ロジックシグナルを発生する。

【0010】図3は、指紋センサ12が列方向の第1の走査線Iを走査した際に、走査セル(1, 13)、

(1, 15)がそれぞれハイ・ロジックシグナルを生じて、他の走査セルがロー・ロジックシグナルを発生したことを示している。図4は、列方向の第2の走査線IIを走査して得られた走査線データを示している。図5は、行方向の第1の走査線IVを走査して得られた走査線データを示している。すなわち、指紋のユニークな特徴を考えると、もしもカード所有者が正当使用者と異なれば指紋走査データも指紋照合データと異なる。

【0011】上述のカードリーダーインターフェース回路13は、作動されてカードリーダー2と通信することができる。

【0012】上述のマイクロプロセッサ14は、指紋センサ12、メモリ装置11及びカードリーダーインターフェース回路13と接続されていて、上記指紋センサ12から指紋走査データを受け、そしてメモリ装置11において指紋走査データと指紋照合データとを比較して、正当使用者が札体18の所有者であると同定すれば、マイクロプロセッサ14がカードリーダーインターフェース回路13を作動して、正当使用者がカード所有者であると確認した状態の下でカードリーダー2を介してホストコンピュータ3とカード情報とを交換する。従って、正当使用者がカード所有者でないと、ICカードを使用することができない。

【0013】上述のバッテリー15は、マイクロプロセッサ14に接続されて、ICカード1に必要な電源を供給する。

【0014】上述の機能キーセット16は、マイクロプロセッサ14に接続されており、ホストコンピュータ3と取引されるカード情報を選択して操作することができる。例えば、機能キーセット16がクレジットカードモードに選択されると、ホストコンピュータ3と取引するカード情報は、クレジットカードナンバーを含んでいる。そして、ネットワーク取引の安全性を高めるため、

正当使用者が札体18の所有者であると確認した状態の下で、マイクロプロセッサ14によってホストコンピュータ3に転送される指紋照合データのセグメントをメモリ装置11に記憶するのがより好ましい。指紋照合データのセグメントは、ホストコンピュータ3と交換したカード情報の期日或いは時間に依じて、選択した走査線データの何れかを選ぶことができ、または走査線データの一つをランダムに選択することもできる。

【0015】ここで、一例を挙げると、指紋照合データの各走査線データに番号を付けて、指紋走査区域Mの列方向の偶数走査ラインの走査データを数"0"に設定して、指紋走査区域Mの列方向の奇数走査ラインの走査データを数"1"に設定し、指紋走査区域Mの行方向の偶数走査ラインの走査データを数"2"に設定して、指紋走査区域Mの行方向の奇数走査ラインの走査データを数"3"に設定する。そして、選択条件が時間2:30であると、カードリーダー2のアクセスから指紋照合データのセグメントが数2, 3, 0の走査線データと対応して、0-2-3-0の順序でホストコンピュータ3に転送され、このホストコンピュータ3が指紋照合データのセグメントと選択時間条件でホストコンピュータ3に記憶された指紋照合データを比較する。他方の例では、選択条件が4:33 5/3/1999の時間と期日であると、カードリーダー2のアクセスにより指紋照合データのセグメントが数0, 1, 3, 4, 9, 5の走査線データと対応して、1-9-9-9-0-5-0-3-0-4-3-3の順序でホストコンピュータ3に転送される。すなわち、指紋照合データのセグメントの機動的交換により特定条件、例えば4:33 5/3/1999の下で妥当なICカードの使用取引行為を安全にする。換言すると、特定時間及び期日で生じるICカード1の転送カード情報が許可なきコピーであるとき、或いはカード情報が他の時間や期日で使用する不当な取引は、結果として、ホストコンピュータ3に拒絶される。

【0016】上述の表示パネル17は、マイクロプロセッサ14とに接続されており、ホストコンピュータ3との交換カード情報を表示するように制御される。この表示パネル17は、ホストコンピュータ3からの、例えば合計金額や収支バランス等をも表示する。

【0017】以上を要約すると、本実施形態の指紋によって識別されるICカードは、ホストコンピュータ3と通信リンクを形成するカードリーダー2によりアクセスされるICカード1であって、札体18と、札体18に設けられて、正当使用者の指紋を走査して得られた指紋照合データ、及びカード情報を記憶するメモリ装置11と、札体18に設けられて、札体18所有者の指紋を走査して指紋走査データを生ずる指紋センサ12と、札体18に設けられて、カードリーダー2と通信するように作動できるカードリーダーインターフェース回路13と、札体18に設けられて、メモリ装置11、指紋セ

ンサ12及びカードリーダーインターフェース回路13と連結し、指紋センサ12から受取った指紋走査データをメモリー装置11で指紋照合データと比較して、札体18の所有者が正当使用者であると確認すれば、カードリーダーインターフェース回路13を作動してカードリーダー2を介してホストコンピュータ3とカード情報を交換するマイクロプロセッサ14とをそれぞれ備えて成るものである。

【0018】

【発明の効果】上記のように構成された本発明によれば、下記のような優れた作用効果を奏することができる。

(1) ICカード1がICカード所有者の指紋を走査して得られた指紋走査データとメモリー装置11の指紋照合データとを比較して、正当使用者が所有者であると確認されると、上記ICカード1は正当使用者だけに使用されるので、ICカード1が紛失或いは置忘れた際に伴う危険性を低減することができる。

(2) ICカード1が時間や期日の関連条件を選択してなる指紋照合データのセグメントを送送できるので、ホストコンピュータ3との交換カード情報を機動的に変化させることができ、従って、インターネット取引の際の安全性を向上させることができる。

(3) ICカード1をバンクカード、身分証明カード或いはクレジットカードとして使用できるので、使用者

は単に1枚のカードだけを携帯して色々な異なる役割を果たすことができ、より便利になる。

【図面の簡単な説明】

【図1】本発明の比較的好ましい実施形態に係るICカードの構成を示す電気回路ブロック図である。

【図2】本発明の実施形態における指紋センサの指紋走査区域を示す図である。

【図3】図2で示した列方向の第1の走査線Iの走査線データを表示する図である。

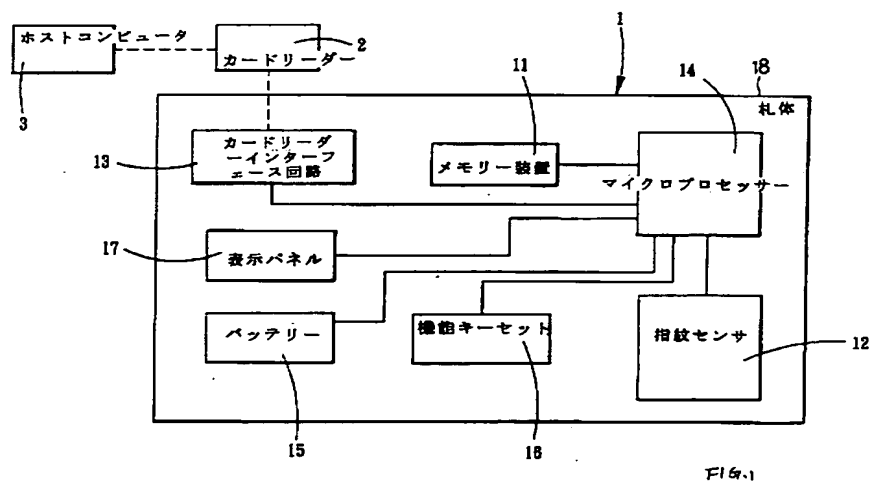
【図4】図2で示した列方向の第2の走査線Iの走査線データを表示する図である。

【図5】図2で示した行方向の第1の走査線Iの走査線データを表示する図である。

【符号の説明】

- 1 ICカード
- 2 カードリーダー
- 3 ホストコンピュータ
- 5 指紋
- 11 メモリー装置
- 12 指紋センサ
- 13 カードリーダーインターフェース回路
- 14 マイクロプロセッサ
- 15 バッテリー
- 16 機能キーセット
- 17 表示パネル
- 18 札体

【図1】



【図2】

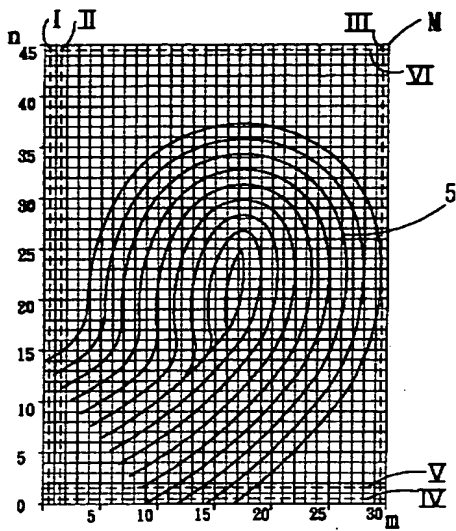


FIG.2

【図5】

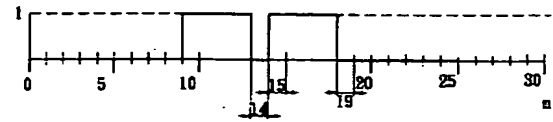


FIG.5

【図3】

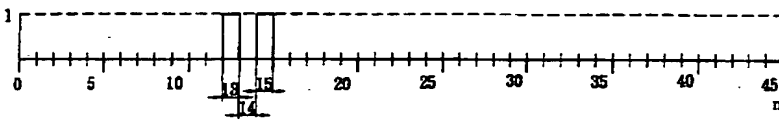


FIG.3

【図4】

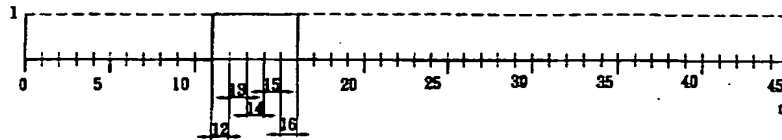


FIG.4